(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－313918
（P2001－313918A）
(43)公開日　平成13年11月9日(2001.11.9)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｎ	7/16		Ｈ０４Ｎ	7/16	Ｚ　５Ｃ０２５
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ａ　５Ｃ０６３
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｆ　５Ｃ０６４
					Ｃ　５Ｊ１０４
Ｈ０４Ｌ	9/08		Ｈ０４Ｎ	5/44	Ａ　９Ａ００１

審査請求　未請求　請求項の数6　ＯＬ　（全 15 頁）　最終頁に続く

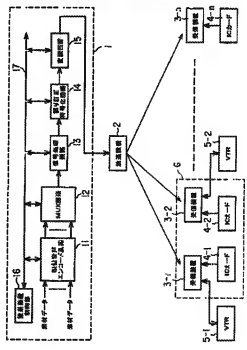
(21)出願番号　特願2000－131390(P2000－131390)
(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　吉田　治
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　有料放送システムと、この有料放送システムで使用される放送装置、受信装置およびセキュリティモジュール

(57)【要約】
【課題】　コピーの配布などの不正は防止した上で、家庭内などの特定の範囲内では記録媒体に記録した番組の再生の自由度を向上させて加入者の便を図る。
【解決手段】　放送装置１は、送信する番組ストリーム中のＥＣＭにグループ記録の許否を示した記録制御情報を含ませる。受信装置３はユーザによりグループ記録が要求された場合、選局された番組ストリームのＥＣＭをＩＣカード４に与える。ＩＣカード４は、ＥＣＭと事前に取得して記憶してあるＥＭＭの情報とからグループ記録の可否を判断し、グループ記録が可能である場合にのみ、複数の契約に対して共通のグループ鍵を用いて暗号化したＥＭＭを生成して受信装置３に返す。受信装置３は、ＩＣカード４からＥＭＭが返されたならば、そのＥＭＭを選局された番組ストリームに挿入して記録用の番組ストリームを作成してこれを番組記録のためにＶＴＲ５へと与える。



【特許請求の範囲】

【請求項１】　放送装置、受信装置およびセキュリティモジュールよりなり、

前記放送装置に設けられ、番組の素材を示す少なくとも一系列の素材情報、番組に関する制御情報を含んだ番組情報、ならびに各有料受信契約毎の個別の制御情報を含んだ個別情報を多重してなる番組ストリームを送信するストリーム送信手段と、

前記放送装置に設けられ、前記ストリーム送信手段が送信する番組ストリーム中にその番組ストリームに関してグループ記録の拒否を示す記録制御情報を含ませる記録制御情報送信手段と、

前記受信装置に設けられ、前記放送装置から送信されて到来した前記番組ストリームに自装置に関する契約についての個別情報が多重されている場合に、この個別情報を自装置に装着された前記セキュリティモジュールへと与える個別情報処理手段と、

前記セキュリティモジュールに設けられ、装着先の前記受信装置から与えられた個別情報に含まれた所定の制御情報を記憶しておく記憶手段と、

前記受信装置に設けられ、前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに多重されている前記番組情報を自装置に装着された前記セキュリティモジュールへと与える番組情報処理手段と、

前記受信装置に設けられ、前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに含まれている前記記録制御情報を自装置に装着された前記セキュリティモジュールへと与える記録制御情報処理手段と、

前記セキュリティモジュールに設けられ、装着先の前記受信装置から与えられた前記番組情報に含まれる制御情報、前記記憶手段により記憶されている制御情報および装着先の前記受信装置から与えられた前記記録制御情報とに基づいて、前記受信装置に到来した番組ストリームのグループ記録の可否を判定する記録可否判定手段と、

前記セキュリティモジュールに設けられ、前記記録可否判定手段によりグループ記録が可能であると判定されたならば、前記記憶手段により記憶された制御情報を用いて個別情報を生成する個別情報生成手段と、

前記セキュリティモジュールに設けられ、前記個別情報生成手段により生成された個別情報を、自装置に関する契約を含む複数の契約に対して共通の所定の暗号鍵を用いて暗号化する暗号化手段と、

前記受信装置に設けられ、前記暗号化手段により暗号化された後の前記個別情報を前記放送装置から送信されて到来した前記番組ストリームに多重して記録用の番組ストリームを生成する記録用ストリーム生成手段とを具備したことを特徴とする有料放送システム。

【請求項２】　前記記録制御情報送信手段は、前記番組情報に前記記録制御情報を含ませるものとし、

かつ前記番組情報処理手段が前記記録制御情報処理手段を兼ねることを特徴とする請求項１に記載の有料放送システム。

【請求項３】　前記ストリーム送信手段は、前記素材情報、前記番組情報、ならびに前記個別情報の他に、未来の放送内容を案内するための所定の番組ガイド情報を多重してなる番組ストリームを送信するものとし、

前記受信装置に設けられ、前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体への記録が指定された場合に、その番組ストリームに含まれている前記番組ガイド情報を自装置に装着された前記セキュリティモジュールへと与える番組ガイド情報処理手段を備え、

前記記録制御情報送信手段は、前記番組ガイド情報に前記記録制御情報を含ませるものとし、

かつ前記前記番組ガイド情報処理手段が前記記録制御情報処理手段を兼ねることを特徴とする請求項１に記載の有料放送システム。

【請求項４】　請求項１に記載の受信装置およびセキュリティモジュールとともに有料放送システムを構成する放送装置であって、

番組の素材を示す少なくとも一系列の素材情報、番組に関する制御情報を含んだ番組情報、ならびに各有料受信契約毎の個別の制御情報を含んだ個別情報を多重してなる番組ストリームを送信するストリーム送信手段と、

このストリーム送信手段が送信する番組ストリーム中にその番組ストリームに関してグループ記録の拒否を示す記録制御情報を含ませる記録制御情報送信手段とを具備したことを特徴とする放送装置。

【請求項５】　請求項１に記載の放送装置およびセキュリティモジュールとともに有料放送システムを構成する受信装置であって、

前記放送装置から送信されて到来した前記番組ストリームに自装置に関する契約についての個別情報が多重されている場合に、この個別情報を自装置に装着された前記セキュリティモジュールへと与える個別情報処理手段と、

前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに多重されている前記番組情報を自装置に装着された前記セキュリティモジュールへと与える番組情報処理手段と、

前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに含まれている前記記録制御情報を自装置に装着された前記セキュリティモジュールへと与える記録制御情報処理手段と、

前記セキュリティモジュールの前記暗号化手段により暗

号化された後の前記個別情報を前記放送装置から送信されて到来した前記番組ストリームに多重して記録用の番組ストリームを生成する記録用ストリーム生成手段とを具備したことを特徴とする受信装置。

【請求項6】　請求項1に記載の放送装置および受信装置とともに有料放送システムを構成するセキュリティモジュールであって、

装着先の前記受信装置から与えられた個別情報に含まれた所定の制御情報を記憶しておく記憶手段と、

前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに含まれている前記記録制御情報を自装置に装着された前記セキュリティモジュールへと与える記録制御情報処理手段と、

装着先の前記受信装置から与えられた前記番組情報に含まれる制御情報、前記記憶手段により記憶されている制御情報および装着先の前記受信装置から与えられた前記記録制御情報とに基づいて、前記受信装置に到来した番組ストリームのグループ記録の可否を判定する記録可否判定手段と、

前記記録可否判定手段によりグループ記録が可能であると判定されたならば、前記記憶手段により記憶された制御情報を用いて個別情報を生成する個別情報生成手段と、

前記個別情報生成手段により生成された個別情報を、自装置に関する契約を含む複数の契約に対して共通の所定の暗号鍵を用いて暗号化する暗号化手段とを具備したことを特徴とするセキュリティモジュール。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、衛星放送、地上波放送、ＣＡＴＶ（ケーブル・テレビジョン）等の放送システムにおいて有料放送を行うための有料放送システムと、この有料放送システムで使用される放送装置、受信装置およびセキュリティモジュールに関する。

【０００２】

【従来の技術】衛星放送、地上波放送、ＣＡＴＶ（ケーブル・テレビジョン）等の放送システムにおいて有料放送を行う場合、１つの契約毎に、その契約に固有のＩＤや暗号鍵を登録したＩＣカードをセキュリティモジュールとして発行することが一般的である。そして受信装置ではこのＩＣカードが装着されている場合にのみ、契約の範囲内で有料放送の受信を行う。すなわち、放送信号は特定の暗号鍵を用いて暗号化されており、正規のＩＣカードが装着された受信装置でしか暗号の解除を行うことができないようにしている。

【０００３】なお、単一の契約者に対して複数のＩＣカードを発行する場合もあるが、この場合はＩＣカードの発行枚数分の対価を徴収するのであって、つまりはＩＣカード１枚に対し必ず１つの契約がなされていることに他ならない。すなわち、有料放送の受信装置を複数所有する契約者は、各受信装置のそれぞれに関して契約したＩＣカードが個々に必要となる。

【０００４】さて、このような有料放送により放送される番組であっても、ビデオテープなどの記録媒体に記録しておいて後で再生することを可能とする場合がある。そしてこの場合には不正なコピーなどを防止するために、暗号化された状態の放送信号を記録する方式が一般的に用いられる。

【０００５】さて、放送信号は例えばＩＳＯ／ＩＥＣ１３８１８－１規格の形式のトランスポートストリームとされる。このトランスポートストリームに含まれる番組の素材データ（映像データや音声データなど）に関する暗号鍵は、不正受信を防止するために周期的に変化される。そして素材データに関する暗号鍵を知るためには、各契約毎の個別情報（以下、ＥＭＭと称する）を参照する必要がある。なおＥＭＭは、各契約に対して設定された固有の暗号鍵（ＩＣカードに登録されるもの）により暗号化された状態でトランスポートストリームに多重されている。

【０００６】ＥＭＭは、多数の契約のそれぞれに関するものが順次伝送される。このためＥＭＭは、１つの契約に関してはある程度長い周期で伝送される。そこで受信装置側では、到来したＥＭＭに含まれる情報をＩＣカード中に記憶しておいて使用することとしている。そして新たにＥＭＭが到来したことに応じて、ＩＣカード中の情報を更新する。

【０００７】このため、記録媒体への記録期間内にはＥＭＭが到来しない場合があり、このようにＥＭＭを含まないトランスポートストリームをそのまま記録媒体に記録したのでは、そのトランスポートストリームに含まれる素材データの暗号解除が行えなくなってしまう。

【０００８】そこでＩＣカードにおいて、記憶してある情報を用いてＥＭＭを生成し、これを各契約に対して設定された固有の暗号鍵を用いて暗号化した上で受信装置側へと与える。受信装置では、このＩＣカードから与えられるＥＭＭを受信したトランスポートストリーム中に挿入することで、記録用のトランスポートストリームを生成して記録に供する。

【０００９】このように、ＩＣカードに登録された契約毎に固有の暗号鍵を使用して暗号化したＥＭＭを多重したトランスポートストリームを記録するので、記録時に使用したＩＣカードが装着された装置でしか再生できない。よってたとえ不正にコピーを行ったとしても再生可能な装置は１台に限定されるので、コピーを配布するような不正は防止される。

【００１０】ところが、家庭内に複数の受信装置やＶＴＲがある場合、ある部屋の装置で記録した番組を別の部屋の装置で再生したり、留守録等で複数の装置を使用する場合など、上述のように再生可能な装置が限定されて

いると、ＩＣカードの交換を行わなければならず、非常に不便であった。また、記録時に使用したＩＣカードを装着した装置が使用中の場合には、他の装置が不使用だったとしてもその装置では再生を行うことができず、非常に不便であった。

【００１１】また、家庭内にある複数のＩＣカードのうちの契約レベルが比較的高いＩＣカードを用いて記録した番組の再生を行っている最中には、新たな番組の受信には契約レベルが比較的低いＩＣカードを使用して行わざるを得ず、新規の番組受信にも制限が加わるという不具合があった。

【００１２】

【発明が解決しようとする課題】以上のように従来は、記録媒体に記録した番組は、記録する際に使用したセキュリティモジュールを装着した装置でのみ再生可能となっているため、家庭内などにおける装置の使用を著しく制限し、加入者に非常に不便を強いるものとなっていた。

【００１３】本発明はこのような事情を考慮してなされたものであり、その目的とするところは、コピーの配布などの不正は防止した上で、家庭内などの特定の範囲内では記録媒体に記録した番組の再生の自由度を向上させて加入者の便を図ることができる有料放送システムと、この有料放送システムで使用される放送装置、受信装置およびセキュリティモジュールを提供することにある。

【００１４】

【課題を解決するための手段】以上の目的を達成するために本発明は、以下に示す構成とした。すなわち、放送装置では、番組の素材を示す少なくとも一系列の素材情報、番組に関する制御情報を含んだ番組情報、ならびに各有料受信契約等の個別の制御情報を含んだ個別情報を多重してなる番組ストリームを、例えば映像音声エンコード回路、多重化回路、信号処理回路、誤り訂正符号化回路および変調回路よりなるストリーム送信手段によって送信するに当り、このストリーム送信手段が送信する番組ストリームに関してグループ記録の拒否を示す記録制御情報を、例えば放送装置制御部のソフトウェア処理により実現される記録制御情報送信手段により前記番組ストリーム中に例えば前記番組情報または番組ガイド情報に含ませることで含ませる。

【００１５】受信装置では、例えば受信装置制御部のソフトウェア処理により実現される個別情報処理手段が、前記放送装置から送信されて到来した前記番組ストリームに自装置に関する契約についての個別情報が多重されている場合に、この個別情報を自装置に装着された例えばＩＣカードなどのセキュリティモジュールへと与える。そうすると前記セキュリティモジュールでは、装着先の前記受信装置から与えられた個別情報に含まれた所定の制御情報を、例えばメモリと制御回路のソフトウェア処理により実現される個別情報記憶制御手段とからなる記憶手段により記憶しておく。

【００１６】前記受信装置では、例えば受信装置制御部のソフトウェア処理により実現されて例えば記録制御情報処理手段としての機能を兼ねる番組情報処理手段が、前記放送装置から送信されて到来した前記番組ストリームの所定の記録媒体へのグループ記録が指定された場合に、その番組ストリームに多重されている前記番組情報（例えば記録制御情報を含む）を自装置に装着された前記セキュリティモジュールへと与える。そうすると前記セキュリティモジュールでは、例えば制御回路のソフトウェア処理により実現される記録可否判定手段が、装着先の前記受信装置から与えられた前記番組情報に含まれる制御情報、前記記憶手段により記憶されている制御情報および装着先の前記受信装置から与えられた前記記録制御情報とに基づいて、前記受信装置に到来した番組ストリームのグループ記録の可否を判定し、ここでグループ記録が可能であると判定されたならば、例えば制御回路のソフトウェア処理により実現される個別情報生成手段が、前記記憶手段により記憶された制御情報を用いて個別情報を生成する。さらに前記セキュリティモジュールでは、例えば制御回路のソフトウェア処理により実現される暗号化手段が、前記個別情報生成手段により生成された個別情報を、自装置に関する契約を含む複数の契約に対して共通の所定の暗号鍵（グループ鍵）を用いて暗号化する。

【００１７】そして前記受信装置では、例えば制御データ挿入部および受信装置制御部のソフトウェア処理により実現される制御データ挿入制御手段により構成される記録用ストリーム生成手段が、前記暗号化手段により暗号化された後の前記個別情報を前記放送装置から送信されて到来した前記番組ストリームに多重して記録用の番組ストリームを生成する。

【００１８】このような手段を講じたことにより、放送装置で番組ストリーム中に示された記録制御情報によりグループ記録の許可が示された番組についてのみ、ユーザの希望に応じてグループ記録が可能となる。このグループ記録は、セキュリティモジュールで生成され、複数の契約に対して共通の所定の暗号鍵を用いて暗号化された個別情報を放送装置から送信されて到来した前記番組ストリームに多重してなる記録用の番組ストリームを記録させることによる。

【００１９】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態につき説明する。

【００２０】本実施形態は、グループ記録をある条件の下に許容するようにしたものである。グループ記録とは、予め同一グループとしてグループ設定がされた複数の受信装置間では、他の受信装置で受信されて記録媒体に記録された番組を他の受信装置で再生することを許容することを示す。

【0021】図1は本実施形態に係る有料放送システムの要部構成および放送装置の要部構成を示すブロック図である。

【0022】この図に示すように本実施形態の有料放送システムは、放送装置1、放送設備2，受信装置3（3-1～3-n）、ICカード4（4-1～4-n）およびビデオテープレコーダ（VTR）5（5-1，5-2）を有してなる。

【0023】放送装置1では、番組の素材データを含む、例えばISO/IEC13818－1規格の形式のトランスポートストリームが生成される。このトランスポートストリームは、例えば周知の衛星放送インフラ、地上波放送インフラ、CATVインフラなどよりなる放送設備2を介して各受信装置3に向けて放送される。

【0024】受信装置3には、有料放送の受信契約毎に発行されるICカード4が装着される。ICカード4は、登録された契約内容に応じた範囲内での番組の受信を受信装置3に対して許可する。受信装置3は、ICカード4により許可された番組のみに関して、図示しないテレビジョン受像機にて再生させたり、記録用のトランスポートストリームを生成して接続されたVTR5へと出力したりする。

【0025】VTR5は、必要に応じて受信装置3に接続されるものであって、受信装置3から与えられるトランスポートストリームをビデオテープに記録する。

【0026】受信装置3は、ユーザのニーズに応じて、放送事業者との契約の下に複数がグループ化される。この図の例では、受信装置3-1と受信装置3-2とがグループGを形成している。なお、受信装置3自体にグループの情報が設定されるわけではなく、ICカード4-1，4-2にグループ用の共通のデスクランブル鍵が設定されることで、これらのICカード4-1，4-2が装着された受信装置3-1，3-2が同一グループに設定される。

【0027】さて放送装置1は、映像音声エンコード回路11、多重化回路（MUX回路）12、信号処理回路13、誤り訂正符号化回路14、変調回路15および放送装置制御部16を有している。

【0028】番組を構成する映像、音声、データなどの複数の素材データは、映像音声エンコード回路11へと与えられ、それぞれ所定の圧縮符号化方式で符号化される。この符号化された素材データは、それぞれMUX回路12に与えられる。一方MUX回路12には、放送装置制御部16が生成する各種の制御データが与えられる。そしてこれらのデータがMUX回路12により多重されて、例えばISO/IEC13818－1規格の形式のトランスポートストリームが生成される。

【0029】このトランスポートストリームは、信号処理回路13でパケット単位で必要に応じてスクランブルされた後、誤り訂正符号化回路14で誤り訂正のための符号化が施される。なお、スクランブルを掛ける必要のないパケットは、信号処理回路13をスルーされる。

【0030】そしてこのように必要な各種の処理が施されたトランスポートストリームは、変調回路15により所定の伝送路を伝送するための変調がなされた上で、放送設備2へと与えられて放送される。

【0031】さて放送装置制御部16は、例えばCPU、ROMおよびRAMなどを有してなるものであり、放送装置としての動作を実現するべく各部を総括制御するための処理をソフトウェア処理により実現する。そしてこの放送装置制御部16が有する制御手段は、番組放送のための処理手段などの周知の一般的な制御手段に加えて、記録制御情報送信手段を備えている。

【0032】この記録制御情報送信手段は、制御データの1つである番組情報（以下、ECMと称する）に、番組ストリームに関してグループ記録の拒否を示す記録制御情報を含ませる。グループ記録の拒否は、放送事業者により番組毎に任意に指定される。なおECMは、各番組に関する視聴情報やデスクランブル鍵などの種々の情報を記述したものであって、パケット化されてトランスポートストリーム中に多重される。

【0033】図2は図1中の受信装置3、ICカード4およびVTR5の要部構成を示すブロック図である。

【0034】この図に示すように受信装置3は、チューナ復調回路21、誤り訂正回路22、信号処理回路23、分離回路（DEMUX回路）24、映像音声デコード回路25、映像音声出力回路26、混合回路27、カード制御部28、コネクタ29、制御データ挿入部30、1394インタフェース31、ユーザインタフェース（ユーザI/F）32および受信装置制御部33を有している。そしてチューナ復調回路21、誤り訂正回路22、信号処理回路23、分離回路（DEMUX回路）24、映像音声デコード回路25、映像音声出力回路26、混合回路27、カード制御部28、コネクタ29、制御データ挿入部30、ユーザインタフェース（ユーザI/F）32および受信装置制御部33は、バス34を介して互いに接続されている。

【0035】図示しないアンテナなどにより放送波を受けて生成された放送波信号が端子T1から入力され、チューナ復調回路21へと与えられる。この放送波信号は、チューナ復調回路21でベースバンドのトランスポートストリームに復調される。この復調されたトランスポートストリームは、誤り訂正回路22で所定の誤り訂正が行われたのち、信号処理回路23に入力される。

【0036】信号処理回路23には、トランスポートストリームに含まれるECMに示されたデスクランブル鍵が受信装置制御部33により設定される。トランスポートストリームは、スクランブルが掛けられているパケットのデスクランブルが信号処理回路23にて行われる。なお、スクランブルが掛けられていないパケットについては、何も処理されずそのまま信号処理回路23をスルーされる。

【００３７】信号処理回路２３から出力されたトランスポートストリームは、ＤＥＭＵＸ回路２４で各コンポーネントに分離され、そのうちの素材データは映像音声デコード回路２５へ、また制御データは受信装置制御部３３へそれぞれ与えられる。

【００３８】素材データは、映像音声デコード回路２５でそれぞれ復号された上で映像音声出力回路２６に与えられ、適宜合成されて番組データが再生される。さらにこの再生された番組データは映像音声出力回路２６にてアナログの番組信号に変換された上で、混合回路２７を介して端子Ｔ２から出力される。端子Ｔ２には例えばテレビジョン受像機（図示せず）などが接続され、このテレビジョン受像機などで番組信号に基づく番組再生が行われる。

【００３９】なお混合回路２７は、メニュー表示をＯＳＤ（On Screen Display）により行うために、受信装置制御部３３から与えられる映像信号を映像音声出力回路２６から出力される番組信号に混合する。

【００４０】ＩＣカード４は、ＩＣカード４に設けられたコネクタ４１がコネクタ２９に挿入されることで受信装置３へと装着される。コネクタ２９にはカード制御部２８が、またコネクタ４１には制御回路４２がそれぞれ接続されている。従って装着状態では、カード制御部２８と制御回路４２との間でのデータの授受により、受信装置３によるＩＣカード４のアクセスが実現される。

【００４１】そこでカード制御部２８は、受信装置制御部３３の制御の下に制御回路４２とのデータの授受を行う。

【００４２】一方、ＶＴＲ５は、このＶＴＲ５に設けられた端子Ｔ１１が端子Ｔ３にケーブルＣを介して接続されることで受信装置３へと接続される。端子Ｔ３および端子Ｔ１１には、受信装置３およびＶＴＲ５のそれぞれに設けられた１３９４インタフェース３１，５１がそれぞれ接続されている。従って接続状態では、１３９４インタフェース３１，５１間でのIEEE 1394に準拠した手順でのデータ転送により、受信装置３とＶＴＲ５との間でのデータの授受が行われる。

【００４３】１３９４インタフェース３１からの受信装置３内側への出力信号線は、誤り訂正回路２２から信号処理回路２３へのデータ転送線に直接的に接続されている。従って１３９４インタフェース３１でＶＴＲ５から取り込まれたデータは、信号処理回路２３へと与えられる。１３９４インタフェース３１への受信装置３内側からの入力信号線は、誤り訂正回路２２から信号処理回路２３へのデータ転送線に制御データ挿入部３０を介して接続されている。従って誤り訂正回路２２から出力されるトランスポートストリームが、制御データ挿入部３０を介して１３９４インタフェース３１へ与えられ、ＶＴＲ５へと出力される。

【００４４】制御データ挿入部３０は、受信装置制御部３３により与えられるＥＭＭを、１３９４インタフェース３１へと伝送されるトランスポートストリーム中に挿入する。

【００４５】ユーザＩ／Ｆ３２には、操作パネルやリモートコントローラ（ともに図示せず）からの信号を端子Ｔ４を介して入力し、ユーザによる指示の内容を認識する。そしてユーザＩ／Ｆ３２は、認識したユーザ指示内容を受信装置制御部３３へと通知する。

【００４６】受信装置制御部３３は、例えばＣＰＵ、ＲＯＭおよびＲＡＭなどを有してなるものであり、受信装置としての動作を実現するべく各部を総括制御するための処理をソフトウェア処理により実現する。そしてこの受信装置制御部３３が有する制御手段は、番組受信のための処理手段などの周知の一般的な制御手段に加えて、個別情報処理手段、番組情報処理手段、および制御データ挿入制御手段を備えている。

【００４７】ここで個別情報処理手段は、ＤＥＭＵＸ回路２４で分離されたＥＭＭを、セキュリティ処理のためにＩＣカード４へと与える。

【００４８】番組情報処理手段は、ＤＥＭＵＸ回路２４で分離されたＥＣＭを、セキュリティ処理のためにＩＣカード４へと与える。

【００４９】そして制御データ挿入制御手段は、トランスポートストリームをＶＴＲ５にて記録する場合に、ＩＣカード４から与えられるＥＭＭを記録するトランスポートストリームへと挿入するように制御データ挿入部３０を制御する。

【００５０】さて、ＩＣカード４の制御回路４２には、メモリ４３が接続されている。このメモリ４３には、契約に係るＩＤ、デスクランブル鍵や暗号鍵など、個別情報（以下、ＥＭＭと称する）に含まれる所定の情報が登録されるとともに、運用上取得される所定の情報を格納するために使用される。なお、グループ設定されている場合には、契約毎の固有の暗号鍵（以下、固有鍵と称する）に加えて、グループに対して割り当てられた暗号鍵（以下、グループ鍵と称する）が登録される。

【００５１】さて制御回路４２は、例えばＣＰＵ、ＲＯＭおよびＲＡＭなどを有してなるものであり、受信装置３での有料放送受信に係るセキュリティ確保のための処理を行う。このようなセキュリティ確保のための各種の処理手段は、有料放送受信に係るユーザ認証などの周知の一般的なものに加えて個別情報記憶制御手段、記録可否判定手段、個別情報生成手段および暗号化手段を有している。

【００５２】ここで個別情報記憶制御手段は、受信装置３で新たに受信されて与えられたＥＭＭが自己宛のものであるならば、メモリ４３に登録された情報をそのＥＭＭに含まれる所定の情報に更新する。

【００５３】記録可否判定手段は、ＥＣＭに含まれる記録制御情報とメモリ４３に記憶されたＥＭＭの情報とに

基づいて、受信装置３に到来した番組ストリームの記録の可否ならびにグループ記録の可否を判定する。

【００５４】個別情報生成手段は、記録可否判定手段により記録が可能であると判定された場合にのみ、メモリ４３に記憶された情報を用いてグループ記録用のＥＭＭを生成する。

【００５５】そして暗号化手段は、個別情報生成手段により生成されたＥＭＭを暗号化する。ただし暗号化手段は、グループ記録が不可であると記録可否判定手段により判定された場合ならびに通常記録が要求されている場合には固有鍵を用いて、またグループ記録が可能であると記録可否判定手段により判定されてかつグループ記録が要求されている場合にはグループ鍵を用いる。

【００５６】ＶＴＲ５は、１３９４インタフェース５１の他に、記録再生機構部５２および制御回路５３を有している。

【００５７】記録再生機構部５２は、例えばテープ駆動機構や磁気ヘッドなどを有して構成されたもので、ビデオテープＴが必要に応じて装填される。そして記録再生機構部５２は、ビデオテープＴに対して、１３９４インタフェース５１を介して与えられるトランスポートストリームを記録する。

【００５８】制御回路５３は、１３９４インタフェース５１および記録再生機構部５２を制御してＶＴＲとしての動作を実現する。

【００５９】次に以上のように構成された有料放送システムの動作につき説明する。

【００６０】まず、番組の視聴を有料とする場合、放送装置１ではＭＵＸ回路１２で生成されたトランスポートストリームに対して、信号処理回路１３でスクランブルを掛ける。

【００６１】このスクランブルはパケット単位で行われる。スクランブルに用いる鍵は、第１鍵ｋｓである。この第１鍵ｋｓは、比較的短い周期で変更される。

【００６２】放送装置制御部１６は、使用中の第１鍵ｋｓをＥＣＭ内に示す。そして放送装置制御部１６は、ＥＣＭに関しては第２鍵ｋｗを用いて暗号化する。この第２鍵ｋｗは、第１鍵ｋｓよりも長い周期で変更される。

【００６３】さらに放送装置制御部１６は、使用中の第２鍵ｋｗをＥＭＭ内に示す。そして放送装置制御部１６は、ＥＭＭに関しては各固有鍵ｋｍｉを用いて暗号化する。

【００６４】さてＥＭＭは、各契約毎に、その契約に関する情報を個別に通知する情報である。放送装置制御部１６は、各契約を対象とするＥＭＭを順次トランスポートストリームに挿入する。

【００６５】ＥＭＭは本来、図３に示すような基本情報Ｉ１からなる。この基本情報Ｉ１は、加入者識別情報（加入者ＩＤ）Ｉ１１と契約設定情報Ｉ１２とからなる。加入者識別情報Ｉ１１は、そのＥＭＭの対象となる契約に対して設定された固有の識別子を示す。契約設定情報Ｉ１２は、加入者識別情報Ｉ１１で特定される契約の内容を示す。ただしこの契約設定情報Ｉ１２は、契約情報に変更がない場合には省略することも可能である。

【００６６】しかし本実施形態で放送装置制御部１６は、契約者から新たにグルーピング登録が要求された場合には、グルーピングする契約に関するＥＭＭに、図３に示すようなグループ設定情報Ｉ２を追加する。

【００６７】グループ設定情報Ｉ２は図３に示すように、グループ識別子Ｉ２１と暗号鍵Ｉ２２とを含む。グループ識別子Ｉ２１は、グループに固有となるように決定された識別子である。暗号鍵Ｉ２２は、グループ識別子Ｉ２１で特定されるグループに含まれる複数の契約での共通使用を許容する暗号鍵、すなわちグループ鍵を示す。

【００６８】さて受信装置３では、トランスポートストリームに含まれるＥＭＭはＤＥＭＵＸ回路２４で抽出され、受信装置制御部３３の制御の下にカード制御部２８を介してＩＣカード４の制御回路４２へと与えられる。

【００６９】制御回路４２はＥＭＭが受信装置３から与えられると、そのＥＭＭが自己の契約に関するものであるか否かの判定、すなわちＥＭＭの正当性の判定を行い、正当なＥＭＭであることが確認されれば、このＥＭＭに含まれる各データによりメモリ４３に記憶されているデータを更新する。これにより、新たに割り当てられたグループ識別子やグループ鍵がＩＣカード４に登録され、以降で使用することができるようになる。

【００７０】同様にして、同一グループＧとしてグルーピングすべき他の契約に関しても同一のグループ識別子およびグループ鍵を示したＥＭＭが与えられる。従って、複数の契約間で共通のグループ識別子およびグループ鍵が共有されることとなり、グルーピング登録が行われる。

【００７１】一方、番組の放送を行うに当って放送装置制御部１６は、その番組に関するＥＣＭを作成してトランスポートストリームに挿入する。

【００７２】ＥＣＭは本来、図４に示すような基本情報Ｉ３からなる。この基本情報Ｉ３は、視聴情報Ｉ３１とデスクランブル鍵Ｉ３２とからなる。視聴情報Ｉ３１は、番組視聴の条件を示す情報や料金情報などを必要に応じて含む。デスクランブル鍵Ｉ３２は、トランスポートストリームをデスクランブルするための鍵である。

【００７３】しかし本実施形態で放送装置制御部１６は、図４に示すような記録制御情報Ｉ４をＥＣＭに追加する。

【００７４】記録制御情報Ｉ４は図４に示すように、記録許否情報Ｉ４１、グループ記録許否情報Ｉ４２および記録許容グループ情報Ｉ４３を含む。記録許否情報Ｉ４１は、ビデオテープＴなどの記録媒体への記録を許容するか否かを示す。グループ記録許否情報Ｉ４２は、グル

ープ記録を許容するか否かを示す。記録許容グループ情報Ｉ４３は、グループ記録を許容するグループのグループ識別子を示す。

【００７５】さて受信装置３では、有料番組を選局した場合には、トランスポートストリームに含まれるＥＣＭはＤＥＭＵＸ回路２４で抽出され、受信装置制御部３３の制御の下にカード制御部２８を介してＩＣカード４の制御回路４２へと与えられる。

【００７６】制御回路４２はＥＣＭが受信装置３から与えられると、そのＥＣＭに示された視聴情報と、ＥＭＭから抽出してメモリ４３に記憶してある契約設定情報とを照合し、これにより自己の契約で視聴可能な番組であるか否かの判断を行う。そして制御回路４２は、その判定結果を受信装置３に対して通知するとともに、視聴可能である場合にはデスクランブル鍵も受信装置３に与える。さらに制御回路４２は、ＥＣＭに記録制御情報が含まれていたならば、この記録制御情報も暗号を解除した状態で受信装置３に与える。

【００７７】受信装置３では、ＩＣカード４より視聴可能である旨が通知されたならば、その通知とともに与えられるデスクランブル鍵を受信装置制御部３３が信号処理回路２３に設定して、トランスポートストリームのデスクランブルを行わせる。これにより、有料番組の視聴が可能となる。また受信装置制御部３３は、記録制御情報が与えられたならば、それを内部メモリに保持しておく。なお、ＩＣカード４より視聴不可能の旨が通知されたのであれば、受信装置制御部３３はその旨をユーザに通知するなどの措置を必要に応じて取る。

【００７８】ところで本実施形態では、番組の記録に関しては、デスクランブルが行われる前のトランスポートストリームを記録する形態をとる。従って、上述のような動作により番組を視聴可能な状態にあっても、そのままでは番組の記録は行えない。

【００７９】さて、ユーザＩ／Ｆ３２を介してユーザから番組記録を行う要求が伝えられたならば、受信装置制御部３３はこれに応じて図５に示すような記録制御処理を実行する。

【００８０】この記録制御処理において受信装置制御部３３はまず、内部メモリに保存してある記録制御情報を確認する（ステップＳＴ１）。すなわち受信装置制御部３３はここで、選局中の番組の記録が許容されているか否か、ならびにグループ記録が可能かどうか、さらには個人記録およびグループ記録のそれぞれでの料金が異なる場合にはそれぞれの料金がいくらであるかなどを判断する。なお個人記録とは、従来通りの単一の受信装置３でのみ記録内容の再生を行える形態での記録のことである。

【００８１】続いて受信装置制御部３３は、上述の判断の結果を示す例えば図６に示すような画像を作成し、これを混合回路２７を介して出力することでテレビジョン受像機などに表示させる。このときの表示形式は、番組の画像に切り替えて表示する形式としても良いし、ＯＳＤによってもよい。

【００８２】図６の例では、番組のタイトル名、録画条件（ここでは、個人記録およびグループ記録の双方が許容されている場合を示す）、料金のそれぞれが示してある。さらに、個人記録およびグループ記録のいずれを実行するか、あるいは番組記録を取りやめるか（キャンセル）のユーザ指定を受け付けるためのボタンＢ１，Ｂ２，Ｂ３を表示してある。

【００８３】そしてこの状態で受信装置制御部３３は、ボタンＢ１，Ｂ２，Ｂ３のいずれかの選択指定がユーザに入力されるのを待ち受け、その入力をチェックする（ステップＳＴ３）。すなわち、個人記録またはグループ記録の開始、もしくは記録の取りやめのいずれかを示す選択情報がユーザＩ／Ｆ３２から入力されると受信装置制御部３３は、保持している情報に沿った正しい入力であるか否かをチェックする。

【００８４】なされた入力が正しいものである場合に受信装置制御部３３は、記録の開始の要求であったか否かを判断し（ステップＳＴ４）、そうではない場合、すなわちキャンセルが指定された場合にはそのまま今回の記録制御処理を終了する。

【００８５】しかしながら記録の開始が要求されたのであれば受信装置制御部３３は、カード制御部２８を駆動してＩＣカード４に契約情報の確認を要求する（ステップＳＴ５）。

【００８６】この要求を受けるとＩＣカード４の制御回路４２は、グループ記録を行うと通知されたのであれば、メモリ４３にグループ識別子およびグループ鍵が設定されているか否かのチェックを行う。そして制御回路４２は、メモリ４３にグループ識別子およびグループ鍵が設定されていない場合にはグループ記録が不可能である旨を通知する応答を、またメモリ４３にグループ識別子およびグループ鍵が設定されている場合にはグループ記録が可能である旨を通知する応答をそれぞれ受信装置３へ返す。

【００８７】そこで受信装置制御部３３はこのようなＩＣカード４からの応答を確認し、ユーザが要求した通りの番組記録が行える か否かの判断を行う（ステップＳＴ６）。ここで、要求通りの番組記録が行えないのであれば受信装置制御部３３は、その旨をユーザに報知するための画像を混合回路２７を介して出力することでテレビジョン受像機などに表示させ（ステップＳＴ７）、この上で今回の記録制御処理を終了する。なお図７は、選局中の番組記録を行うのに必要なグルーピング登録がなされていない場合に表示する画像例である。

【００８８】これに対して要求通りの番組記録が行えるのであれば受信装置制御部３３は、行うべきが個人記録およびグループ記録のいずれであるかを判断する（ステ

ップＳＴ８）。そして個人記録を行うべきであれば個人記録用のＥＭＭの生成を（ステップＳＴ９）、またグループ記録を行うべきであればグループ記録用のＥＭＭの生成を（ステップＳＴ１０）、それぞれＩＣカード４に対して要求する。

【００８９】このようにして記録用のＥＭＭの生成が要求されるとＩＣカード４にて制御回路４２は、メモリ４３に記憶してあるデータを用いてＥＭＭを生成する。そして個人記録用が要求されている場合には固有鍵を用いて、またグループ記録用が要求されている場合にはグループ鍵を用いて、上記生成したＥＭＭを暗号化する。そして制御回路４２は、この暗号化した後のＥＭＭを受信装置３へと与える。

【００９０】そこで受信装置制御部３３は、上述のようにしてＩＣカード４から与えられるＥＭＭを制御データ挿入部３０へと与え、トランスポートストリームのＮＵＬＬパケット部分へ挿入させる（ステップＳＴ１１）。そしてこののちに受信装置制御部３３は、今回の記録制御処理を終了する。

【００９１】制御データ挿入部３０でＥＭＭが挿入されたトランスポートストリームは、１３９４インタフェース３１でフォーマット変換された後に端子Ｔ３からスクランブルが施されたままの状態で出力される。

【００９２】ＶＴＲ５では、受信装置３の端子Ｔ３から出力されてケーブルＣを介して電送されてきたトランスポートストリームを１３９４インタフェース５１にて取り込み、記録再生機構部５２によってビデオテープＴに記録する。

【００９３】かくして、ＶＴＲ５にはＩＣカード４で生成されたＥＭＭが挿入されたトランスポートストリームが出力されることとなり、このトランスポートストリームがビデオテープＴに記録される。

【００９４】一方、ビデオテープＴに記録されたトランスポートストリームに基づく番組視聴のための動作は以下の通りである。

【００９５】まず、ビデオテープＴに記録されたトランスポートストリームは記録再生機構部５２により読み出され、１３９４インタフェース５１を介して受信装置３へとケーブルＣを介して与えられる。

【００９６】受信装置３では、このようにしてＶＴＲ５より与えられたトランスポートストリームは、１３９４インタフェース３１で取り込まれて、そのまま信号処理回路２３へと与えられる。そしてこのＶＴＲ５より与えられたトランスポートストリームに基づく番組再生は放送受信時と同様にして行われるのであるが、この際に用いられるＥＭＭは記録時にＩＣカード４にて生成されたものである。

【００９７】このＥＭＭが固有鍵を用いて暗号化されているのだとするとその暗号の解除は、番組記録時にトランスポートストリームの受信を行った受信装置３に装着されていたＩＣカード４のみである。従って、番組記録時に用いたのと同一のＩＣカード４が受信装置３に装着されている場合にのみ、受信装置３はデスクランブル鍵を取得することができ、番組再生を行うことができる。

【００９８】これに対してＥＭＭがグループ鍵を用いて暗号化されているのだとするとその暗号の解除は、番組記録時にトランスポートストリームの受信を行った受信装置３に装着されていたＩＣカード４と同一のグループとしてグルーピング登録されたカードのみである。従って、番組記録時に用いたのとは異なるＩＣカード４が受信装置３に装着されている場合であっても、その装着されたＩＣカード４が番組記録時に用いたものと同一のグループとしてグルーピング登録されたものである場合に限って番組再生を行うことができる。

【００９９】このように本実施形態によれば、複数のＩＣカード４に対して共通のグループ鍵を登録しておき、グループ記録の際には記録するトランスポートストリームに対して、グループ鍵を用いて暗号化したＥＭＭを挿入する。従って、グループ記録されたトランスポートストリームに基づく番組再生は、共通のグループ鍵が登録された複数のＩＣカード４が装着された受信装置３のいずれでも行うことができる。この結果、ＩＣカード４の交換を行うことなしに、番組記録を行ったのとは異なる受信装置３を用いての視聴が可能であり、ユーザの便が大幅に向上する。すなわち例えば、ある家庭に複数の受信装置３が存在するならば、それらの受信装置３に関するそれぞれの契約をグルーピング登録しておくことにより、ある部屋で記録した番組を別の部屋で視聴することが可能となり、ユーザの視聴形態の自由度が高くなる。

【０１００】しかも本実施形態では、グループ記録されたものであっても、その視聴範囲は同一のグルーピング登録が行われた範囲内に制限されるので、コピーの配布のような不正は防止することができ、セキュリティは十分に保たれる。

【０１０１】さらに本実施形態によれば、グルーピング登録が行われた契約でしかグループ記録が有効利用できないので、放送事業者側はグルーピング登録を不可サービスとして対価を回収することも可能である。

【０１０２】さらに本実施形態によれば、記録制御情報Ｉ４を放送装置１から受信装置３へと通知するためにＥＣＭを利用しているので、番組放送中は数１００ｍｓから数秒のオーダーで頻繁に記録制御情報Ｉ４の通知がなされる。従って、受信装置３では番組放送中の如何なるタイミングでも即座に記録制御情報Ｉ４を取得することができ、番組記録が必要になったときにグループ記録の可否をリアルタイムに判断することが可能となる。

【０１０３】なお、本発明は上記実施形態に限定されるものではない。例えば上記実施形態では、記録制御情報Ｉ４をＥＣＭに含ませて放送装置１から受信装置３へと通知するようにしているが、例えばＥＩＴ（Event Info

rmation Table）やＳＤＴ（Service Definition Table）などの番組ガイドを構成する制御情報に含ませるようにしても良い。図８はＥＩＴに記録制御情報Ｉ４を含ませた様子を示す図である。この図において、符号Ｉ５を付して示すものがＥＩＴの基本情報である番組構成要素情報であり、これに付加するように記録制御情報Ｉ４を含ませている。

【０１０４】このように番組ガイド情報に記録制御情報Ｉ４を含ませるようにすれば、番組の放送開始前にグループ記録の可否の判定を行うことができ、例えばタイマ記録の予約時に記録方法を選択することが可能となる。

【０１０５】ただしこの場合には、番組の放送開始前にＩＣカード４から記録用のＥＭＭが与えられることになるので、そのＥＭＭを実際に番組が放送されるまで受信装置３で記憶保持しておく。あいは、ユーザからの記録要求を番組放送開始まで受信装置３で保持しておき、放送開始時や放送開始直前に放送装置１からＩＣカード４へＥＭＭを要求するようにしてもよい。

【０１０６】なお、ＥＩＴ等の番組ガイド情報はリアルタイム性はないが全時間帯で取得可能な情報であり、ＥＣＭは番組放送中は短い周期でリアルタイムに取得可能な情報であるので、それらの制御情報の双方で記録制御情報Ｉ４の通知を行うようにすることで、予約時から番組放送中まで如何なる時にもスムースな記録制御が行得るようになる。

【０１０７】また記録制御情報Ｉ４は、ＥＣＭ、ＥＩＴ、ＳＤＴ以外の既存の制御情報に含ませるようにしても良いし、あるいは記録制御情報Ｉ４を通知するための専用の制御データを設定してこれを適当なパケットとして伝送するようにしても良い。

【０１０８】また上記実施形態では、受信装置３は別体のＶＴＲ５へと記録用のトランスポートストリームを出力してビデオテープＴへの記録をＶＴＲ５に行わせるものとしているが、ＶＴＲ５の機能を受信装置３に内蔵していても良い。

【０１０９】また上記実施形態では、番組を記録するための記録媒体としてビデオテープＴを例示しているが、ＤＶＤなど記録媒体の種類は任意であって良い。

【０１１０】このほか、本発明の要旨を逸脱しない範囲で種々の変形実施が可能である。

【０１１１】

【発明の効果】本発明によれば、放送装置で番組ストリーム中に示された記録制御情報によりグループ記録の許可が示された番組についてのみ、ユーザの希望に応じてグループ記録を可能とすることとし、かつグループ記録は、セキュリティモジュールで生成され、複数の契約に対して共通の所定の暗号鍵を用いて暗号化された個別情報を放送装置から送信されて到来した前記番組ストリームに多重してなる記録用の番組ストリームを記録させることにより実現するようにしたので、コピーの配布などの不正は防止した上で、家庭内などの特定の範囲内では記録媒体に記録した番組の再生の自由度を向上させて加入者の便を図ることが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る有料放送システムの要部構成および放送装置の要部構成を示すブロック図。

【図２】図１中の受信装置３、ＩＣカード４およびＶＴＲ５の要部構成を示すブロック図。

【図３】本発明の一実施形態で使用するＥＭＭのデータ構造を模式的に示す図。

【図４】本発明の一実施形態で使用するＥＣＭのデータ構造を模式的に示す図。

【図５】図１注の受信装置制御部３３による記録制御処理の際の処理手順を示すフローチャート。

【図６】番組記録に関する情報をユーザに提示するための表示画像の一例を示す図。

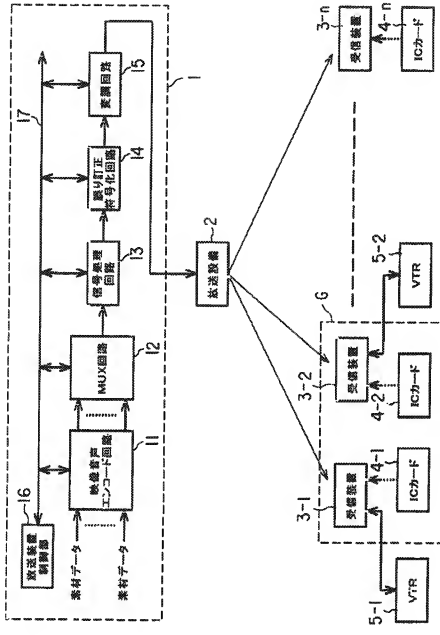
【図７】グループ記録を行うことができない旨をユーザに対して通知するための表示画像の一例を示す図。

【図８】記録制御情報をＥＩＴに含ませた例を示す図。

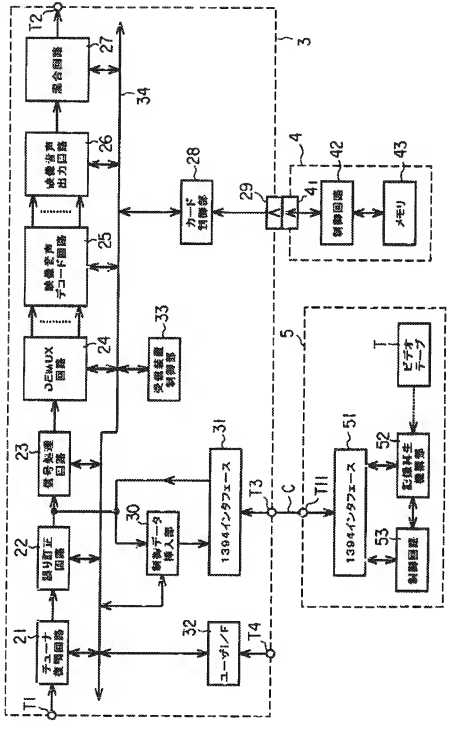
【符号の説明】

１…放送装置、３…受信装置、４…ＩＣカード、１１…映像音声エンコード回路、１２…多重化回路（ＭＵＸ回路）、１３…信号処理回路、１４…誤り訂正符号化回路、１５…変調回路、１６…放送装置制御部、３０…制御データ挿入部、３３…受信装置制御部、４２…制御回路、４３…メモリ、Ｔ…ビデオテープ。

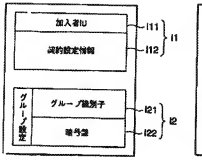
【図1】


送信装置制御部
素材データ
素材データ
映像音声エンコード回路
MUX回路
信号処理回路
高ﾚﾍﾞﾙ圧縮符号化回路
変調回路
放送設備
受信装置
ICカード
VTR
G

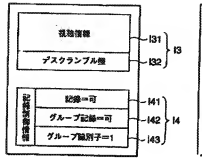
【図2】


T1
T2
T3
T4
T11
T
C
3
4
5
21
チューナ復号回路
22
誤り訂正回路
23
復号処理回路
24
DEMUX回路
25
映像音声デコード回路
26
映像音声出力回路
27
混合回路
28
カードI/F制御部
29
30
制御データ挿入部
31
1394インタフェース
32
ユーザI/F
33
受信装置制御部
34
41
42
制御回路
43
メモリ
51
1394インタフェース
52
記録再生機構部
53
制御回路
ビデオテープ

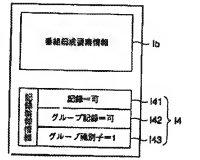
【図3】


加入者ID
I11
契約設定情報
I12
I1
グループ設定
グループ識別子
I21
暗号鍵
I22
I2

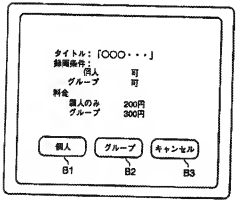
【図4】


視物情報
I31
デスクランブル性
I32
I3
記録装置管理情報
記録=可
I41
グループ記録=可
I42
グループ識別子=1
I43
I4

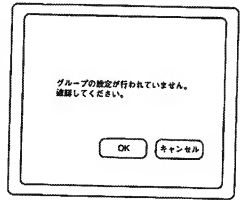
【図8】


番組配信課情報
Ib
記録装置管理情報
記録=可
I41
グループ記録=可
I42
グループ識別子=1
I43
I4

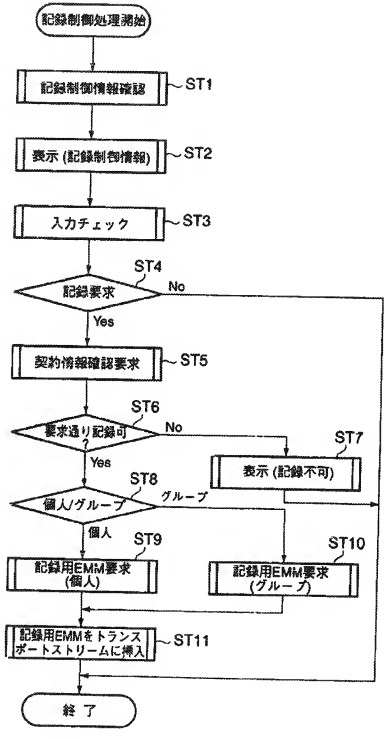
【図6】


タイトル:「OOO・・・」
録画条件:
個人 可
グループ 可
料金
個人のみ 200円
グループ 300円
個人
グループ
キャンセル
B1
B2
B3

【図7】


グループの設定が行われていません。
確認してください。
OK
キャンセル

【図5】


記録制御処理開始
記録制御情報確認
ST1
表示(記録制御情報)
ST2
入力チェック
ST3
ST4
記録要求
No
Yes
契約情報確認要求
ST5
ST6
要求通り記録可?
No
ST7
表示(記録不可)
Yes
ST8
個人/グループ
グループ
個人
ST9
ST10
記録用EMM要求(個人)
記録用EMM要求(グループ)
記録用EMMをトランスポートストリームに挿入
ST11
終了

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI			(参考)
H04N	5/44	H04N	5/44	Z	
		H04L	9/00	601C	
	7/025	H04N	7/08	A	
	7/03				
	7/035				

Fターム(参考) 5C025 AA25 AA30 BA25 BA27 BA30
CB07 CB10 DA01 DA05 DA10
5C063 AA20 AB03 AB07 AC01 AC05
AC10 CA11 CA40 DA20
5C064 BA01 BB01 BB02 BC06 BC16
BC20 BC22 BC25 BC27 BD09
5J104 AA01 AA16 AA32 BA03 EA02
EA17 NA02 NA35 NA41 PA05
9A001 BB03 CC05 DD13 EE03 HH35
JJ71 KK56 KK62 LL03 LL07
LL09

ENGLISH TRANSLATION

Japanese Kokai Patent Application No. 2001-313918

(19) JAPANESE PATENT OFFICE (JP)

(12) KOKAI TOKUHYO PATENT JOURNAL (A)

(11) PATENT APPLICATION PUBLICATION NO. 2001-313918

(43) Publication Date: November 9, 2001

(51) Int. Cl.[7]:	Identification Codes	FI		Theme Codes (Reference)
H 04 N 7/16		H 04 N 7/16	Z	5C025
G 09 C 1/00	660	G 09 C 1/00	660 A	5C063
H 04 H 1/00		H 04 H 1/00	F	5C064
			C	5J104
H 04 L 9/08		H 04 N 5/44	A	9A001

Examination Request: Not filed

No. of Claims: 6 (Total of 15 pages; OL)

Continued on last page

(21) Filing No.: 2000-131390

(22) Filing Date: April 28, 2000

(71) Applicant: 000003078
Toshiba Corporation
1-1 Shibaura, Minato-ku Tokyo

(72) Inventor: Osamu Yoshida
Toshiba Corporation, Yokohama Works
8, Shinsugita-cho, Isogo-ku
Yokohama-shi, Kanagawa-ken

(74) Agent: 100058479
Takahisa Suzue, Patent Attorney
(and 6 others)

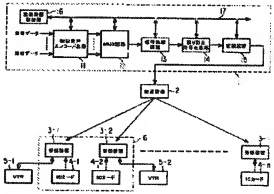
Continued on last page

(54) [Title] CONDITIONAL ACCESS SYSTEM, AND BROADCAST DEVICE, RECEPTION DEVICE AND SECURITY MODULE USED WITH SAME

(57) Abstract

Problem To improve the degree of freedom with respect to reproduction of programs recorded on a recording medium within a prescribed region such as a home, and to ensure convenience for the subscriber, while preventing abuse such as the distribution of copies.

Means to solve A broadcast device 1 causes recording control information – indicating whether group recording is permitted – to be included in the ECM in a program stream to be transmitted. When group recording has been requested by the user, a reception device 3 supplies the ECM for the selected program stream to an IC card 4. Based on the ECM and previously obtained and stored EMM information, IC card 4 judges whether group recording is permitted and – only when group recording is possible – generates and returns to reception device 3 the EMM that is encoded using a group key that is shared with respect to multiple contracts. When the EMM is returned from IC card 4, reception device 3 inserts that EMM into the selected program stream to create a program stream for recoding use, which then is supplied to a VTR 5 for recording of the program.



[Figure is translated at the end of the document.]

[There are no amendments to this patent.]

Claims

1. A conditional access system characterized in that it is comprised of a broadcast device, a reception device, and a security module, and is equipped with

a stream transmission means that is provided in the aforementioned broadcast device and that transmits a program stream formed by multiplexing at least a series of subject matter information that indicates the subject matter for a program, and program information that includes control information pertaining to the program, and individual information that includes individual control information for each conditional access reception contract;

a recording control information transmission means that is provided in the aforementioned broadcast device and that causes recording control information that indicates whether group recording is permitted for the program stream to be included in the program stream transmitted by the aforementioned stream transmission means;

an individual information processing means that is provided in the aforementioned reception device and that, when individual information for the contract pertaining to this same device is multiplexed in the aforementioned transmitted program stream arriving from the aforementioned broadcast device, supplies this individual information to the aforementioned security module installed in this same [reception] device;

a storage means that is provided in the aforementioned security module and that stores prescribed control information that is included in the individual information supplied from the aforementioned reception device in which it is installed;

a program information processing means that is provided in the aforementioned reception device and that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned program information that is multiplexed in that program stream to the aforementioned security module installed in this same [reception] device;

a recording control information processing means that is provided in the aforementioned reception device and that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned recording control information included in that program stream to the aforementioned security module installed in this same [reception] device;

a recording permissibility judgment means that is provided in the aforementioned security module and that, based on the control information included in the aforementioned program information supplied from the aforementioned reception device in which [this security module is] installed, and the control information stored in the aforementioned storage means, and the aforementioned recording control information supplied from the aforementioned reception

device in which [this security module is] installed, judges whether group recording of the program stream that has arrived at the aforementioned reception device is permitted;

an individual information generation means that is provided in the aforementioned security module and that, when the aforementioned recording permissibility judgment means has judged that group recording is possible, generates individual information using the control information stored by the aforementioned storage means;

an encoding means that is provided in the aforementioned security module and that uses a prescribed encoding key that is shared by multiple contracts including the contracts pertaining to this same device to decode the individual information generated by the aforementioned individual information generation means;

and a recording stream generation means that is provided in the aforementioned reception device and that generates a program stream used for recording by multiplexing the aforementioned individual information, after it has been encoded by the aforementioned encoding means, with the aforementioned transmitted program stream arriving from the aforementioned broadcast device.

2. The conditional access system recorded in Claim 1, characterized in that the aforementioned recording control information transmission means causes the aforementioned recording control information to be included in the aforementioned program information,

and the aforementioned program information processing means also serves as the aforementioned recording control information processing means.

3. The conditional access system recorded in Claim 1, characterized in that the aforementioned stream transmission means transmits a program stream formed by multiplexing prescribed program guide information for the purpose of introducing future broadcast content in addition to the aforementioned subject matter information, the aforementioned program information, and the aforementioned individual information,

and [the conditional access system is] equipped with a program guide information processing means that is provided in the aforementioned reception device and that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned program guide information included in that program stream to the aforementioned security module installed in this same [reception] device,

and the aforementioned recording control information transmission means causes the aforementioned recording control information to be included in the aforementioned program guide information,

and the aforementioned program guide information processing means also serves as the aforementioned recording control information processing means.

4. A broadcast device that forms a conditional access system together with the reception device and the security module recorded in Claim 1,

the broadcast device being characterized in that it is equipped with a stream transmission means that transmits a program stream formed by multiplexing at least a series of subject matter information that indicates the subject matter for a program, and program information that includes control information pertaining to the program, and individual information that includes individual control information for each conditional access reception contract;

and a recording control information transmission means that causes recording control information that indicates whether group recording is permitted for the program stream to be included in the program stream transmitted by the aforementioned stream transmission means.

5. A reception device that forms a conditional access system together with the broadcast device and the security module recorded in Claim 1,

the reception device being characterized in that it is equipped with an individual information processing means that, when individual information for the contract pertaining to this same device is multiplexed in the aforementioned transmitted program stream arriving from the aforementioned broadcast device, supplies this individual information to the aforementioned security module installed in this same [reception] device;

a program information processing means that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned program information that is multiplexed in that program stream to the aforementioned security module installed in this same [reception] device;

a recording control information processing means that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned recording control information included in that program stream to the aforementioned security module installed in this same [reception] device;

and a recording stream generation means that generates a program stream used for recording by multiplexing the aforementioned individual information, after it has been encoded by the aforementioned encoding means, with the aforementioned transmitted program stream arriving from the aforementioned broadcast device.

6. A security module that forms a conditional access system together with the broadcast device and the reception device recorded in Claim 1,

the security module being characterized in that it is equipped with a storage means that stores prescribed control information that is included in the individual information supplied from the aforementioned reception device in which it is installed;

a recording control information processing means that, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, supplies the aforementioned recording control information included in that program stream to the aforementioned security module installed in this same device [sic];

a recording permissibility judgment means that, based on the control information included in the aforementioned program information supplied from the aforementioned reception device in which [this security module is] installed, and the control information stored in the aforementioned storage means, and the aforementioned recording control information supplied from the aforementioned reception device in which [this security module is] installed, judges whether group recording of the program stream that has arrived at the aforementioned reception device is permitted;

an individual information generation means that, when the aforementioned recording permissibility judgment means has judged that group recording is possible, generates individual information using the control information stored by the aforementioned storage means;

and an encoding means that uses a prescribed encoding key that is shared by multiple contracts including the contracts pertaining to this same device to decode the individual information generated by the aforementioned individual information generation means.

Detailed explanation of the invention

[0001]

Technical field of the invention

The present invention pertains to a conditional access system for the purpose of performing conditional access broadcasting in a broadcast system for satellite broadcasting, terrestrial broadcasting, CATV (Cable Television), or the like, and pertains to a broadcast device, a reception device, and a security module used in this conditional access system.

[0002]

Prior art

When conditional access broadcasting is performed in a broadcast system for satellite broadcasting, terrestrial broadcasting, CATV (Cable Television), or the like, typically for each individual contract an IC card on which is registered an ID and an encoding key unique to that contract is issued as a security module. In addition, conditional access broadcasting is performed in the reception device, within the scope of the contract, only when this IC card is installed. In other words, the broadcast signal is encoded using a specific encoding key, and the encoding can be released only with a reception device in which a legitimate IC card is installed.

[0003]

In some cases multiple IC cards are issued to a single contractee, but in this case the price is levied for the number of IC cards issued; in other words, there always is one contract with respect to one IC card. In other words, a contractee possessing multiple conditional access reception devices must have a separate contracted IC card for each reception device.

[0004]

In addition, with a program that is broadcast by means of conditional access broadcasting there are cases in which it is possible to record the program to a videotape or the like recording medium, and to reproduce the program later. In this case, to prevent unauthorized copying and the like, typically a system is used whereby the broadcast signal is recorded in the encoded state.

[0005]

The broadcast signal is, for example, a transport stream in the ISO/IEC 13818-1 standard format. The encoding key for the subject matter data (video data, audio data, and the like) for a program included in this transport stream is changed periodically to prevent unauthorized reception. In addition, to know the encoding key for the subject matter data it is necessary to reference the individual information (hereinafter, 'EMM') for each contract. The EMM is multiplexed in the transport stream in the encoded state by means of a unique encoding key (which is registered on an IC card) that is set with respect to each contract.

[0006]

The EMM for each of many contracts is transmitted sequentially; therefore, the EMM for [any] one contract is transmitted at a relatively long interval. Therefore, at the reception device the information included in the EMM that has arrived is stored on an IC card and then is used. When new EMM arrives, the information on the IC card is updated.

[0007]

Therefore, in some cases the EMM does not arrive during the period in which recording to a recording medium is occurring, and thus a transport stream that does not contain the EMM is recorded to the recording medium, so the encoding of the subject matter data included in that transport stream cannot be released.

[0008]

Therefore, the EMM is generated using information stored in the IC card and this [EMM] is supplied to the reception device side while encoded using a unique encoding key set for each contract. By inserting the EMM supplied from this IC card into the received transport stream in the reception device, a transport stream for recording use is generated and provided for recording.

[0009]

Thus, a transport stream – in which is multiplexed EMM that has been encoded using an encoding key that is unique for each contract registered on the IC card – is recorded, so when recording occurs, [the program] can be reproduced only at the device in which the IC card used at the time of recording is installed. Thus, for example, even if unauthorized copying has occurred, there is only one device capable of reproducing [the program], thus preventing abuse such as the distribution of copies.

[0010]

However, when there are multiple reception devices or VTRs in a home and multiple devices are used, such as when a program recorded in one room is reproduced in another room or when unattended recording occurs, then as described above when the device with which reproduction is possible is restricted, the IC card must be exchanged, which is extremely inconvenient. Furthermore, when the device in which the IC card used at the time of recording is installed is in use, even if another device is not in use, that device is unable to reproduce [a program], which is extremely inconvenient.

[0011]

Furthermore, there is a problem in that when a program that was recorded using an IC card that is [one] of the multiple IC cards in the home and that has a relatively high contract level is being reproduced, an IC card with a relatively low contract level must be used to receive a new program, which restricts the reception of new programs.

[0012]

Problems to be solved by the invention

As described above, conventionally a program recorded on a recording medium can be reproduced only on the device in which the security module used at the time of recording is installed, so the use of the device in the home or the like is severely restricted, which greatly inconveniences the subscriber.

[0013]

The present invention was devised in consideration of such circumstances, the objective being to provide a conditional access system that is capable of improving the degree of freedom of the reproduction of programs recorded on a recording medium within a prescribed region, such as a home, and to ensure convenience for the subscriber, while preventing abuse such as the distribution of copies; in addition, the objective is to provide a broadcast device, a reception device, and a security module used with this conditional access system.

[0014]

Means to solve the problems

To achieve the aforementioned objectives, the present invention has the configuration shown in the following. In other words, when the broadcast device transmits – by means of a stream transmission means comprised of a video/audio encoding circuit, a multiplexing circuit, a signal-processing circuit, an error correction/encoding circuit, and a modulation circuit, for example – a program stream formed by multiplexing at least a series of subject matter information that indicates the subject matter for a program, and program information that includes control information pertaining to the program, and individual information that includes individual control information for each conditional access reception contract, [at this time] recording control information indicating whether group recording with respect to the program stream transmitted by the stream transmission means is permitted is included in the aforementioned program stream – for example, in the aforementioned program information or program guide information – by means of a recording control information transmission means that is implemented by software processing in the broadcast device control unit, for example.

[0015]

At the reception device, when individual information for the contract pertaining to this same device is multiplexed in the aforementioned transmitted program stream arriving from the aforementioned broadcast device, for example, an individual information processing means that is implemented by software processing in the reception device control unit supplies this individual information to an IC card or the like security module installed in this same device. Then, at the aforementioned security module, prescribed control information included in the individual information supplied from the aforementioned reception device in which [this security module is] installed is stored in a storage means comprised of an individual information storage control means implemented by means of software processing in a memory control circuit, for example.

[0016]

At the aforementioned reception device, when group recording of the aforementioned transmitted program stream arriving from the aforementioned broadcast device to a prescribed recording medium has been specified, a program information processing means that is implemented by means of software processing in the reception device control unit, for example, and that also serves as a recording control information processing means, for example, supplies the aforementioned program information (which includes recording control information, for example) that is multiplexed in that program stream to the aforementioned security module installed in this same [reception] device. Then, at the aforementioned security module, a recording permissibility judgment means implemented by means of software processing in a control circuit judges whether group recording is permitted for the program stream that has arrived at the aforementioned reception device, [said judgment being] based on the control information included in the aforementioned program information supplied from the aforementioned reception device in which [this security module is] installed, and the control information stored in the aforementioned storage means, and the aforementioned recording control information supplied from the aforementioned reception device in which [this security module is] installed. If it is judged that group recording is possible, an individual information generation means implemented by means of software processing in a control circuit, for example, uses the control information stored in the aforementioned storage means to generate individual information. Furthermore, at the aforementioned security module, an encoding means implemented by means of software processing in a control circuit uses a prescribed encoding key (group key) that is shared by multiple contracts including the contracts pertaining to this same device to decode the individual information generated by the aforementioned individual information generation means.

[0017]

Then, at the aforementioned reception device, a recording stream generation means – which is formed by means of a control data insertion unit and a control data insertion control means that is implemented by means of software processing in the reception device control unit – generates a program stream for recording use by multiplexing the aforementioned individual information, after it has been encoded by the aforementioned encoding means, with the aforementioned transmitted program stream arriving from the aforementioned broadcast device.

[0018]

By implementing such means, group recording is enabled according to the user's desire only for programs for which it is indicated – by means of the recording control information

indicated in the program stream at the broadcast device – that group recording is permitted. This group recording is performed by recording a recording-use program stream formed by multiplexing the individual information – which is generated by the security module and has been encoded using a prescribed encoding key that is shared by multiple contracts – with the aforementioned program stream transmitted from the broadcast device.

[0019]

Embodiment of the invention

In the following an embodiment of the present invention will explained with reference to figures.

[0020]

The embodiment of the present invention permits group recording under certain conditions. Group recording means the permitting of the reproduction of a program, which has been received and recorded on a recording medium by another reception device, on another [sic] reception device, [this being permitted] among multiple reception devices that have been set in advance as [belonging to] the same group.

[0021]

Figure 1 is a block diagram showing the configuration of the relevant parts of a conditional access system and the relevant parts of a broadcast device according to the present embodiment.

[0022]

As shown in this figure, the conditional access system of the present embodiment has a broadcast device 1, a broadcast facility 2, reception devices 3 (3-1 to 3-n), IC cards 4 (4-1 to 4-n), and videotape recorders (VTRs) 5 (5-1, 5-2).

[0023]

At broadcast device 1 a transport stream that includes subject matter data for programs and has the ISO/IEC 13818-1 standard format, for example, is generated. This transport stream is transmitted to each reception device 3 via broadcasting facility 2, which is comprised of a publicly known satellite broadcast infrastructure, terrestrial broadcast infrastructure, CATV infrastructure, or the like.

[0024]

An IC card 4, [one of] which is issued for each conditional access reception contract, is installed in [each] reception device 3. IC card 4 permits a reception device 3 to receive programs within a range that is in accordance with registered contractual content. Reception device 3 reproduces only the programs permitted by IC card 4 on a television receiver, not shown in the figure, or generates a recording-use transport stream that is output to a connected VTR 5.

[0025]

VTR 5 is connected to reception device 3 as needed, recording the transport stream supplied from reception device 3 to videotape.

[0026]

Multiple reception devices 3 can be grouped together according to the user's needs and based on the contract with the broadcasting company. With the example in this figure, reception device 3-1 and reception device 3-2 form a group G. The group information is not set in the reception device 3 itself; instead, the reception devices 3-1 and 3-2 in which IC cards 4-1 and 4-2 are installed are set in the same group by setting a shared descramble key for group use in these IC cards 4-1 and 4-2.

[0027]

Broadcast device 1 has a video/audio encoding circuit 11, a multiplexing circuit (MUX circuit) 12, a signal-processing circuit 13, an error correction/encoding circuit 14, a modulation circuit 15, and a broadcast device control unit 16.

[0028]

The multiple [types of] subject matter data such as video, audio, and [other] data that form a program are supplied to video/audio encoding circuit 11 and are encoded with the respective prescribed compression encoding method. These encoded subject matter data are separately supplied to MUX circuit 12. MUX circuit 12 also is supplied with various types of control data generated by broadcast device control unit 16. These data are multiplexed by MUX circuit 12 and a transport stream is generated in the ISO/IEC 13818-1 standard format, for example.

[0029]

After this transport stream is scrambled as needed in units of packets by signal-processing circuit 13, it undergoes encoding in error correction/encoding circuit 14 for the

purpose of error correction. Packets that are not required to be scrambled are [passed] through signal-processing circuit 13 [as is].

[0030]

Then, this transport stream that has undergone various required processes is modulated by modulation circuit 15 for the purpose of transmission on a prescribed transmission path, and then is supplied to broadcast facility 2 and is broadcast.

[0031]

Broadcast device control unit 16 has a CPU, ROM, RAM, and the like, for example, and implements processes for the overall control of each unit in order to operate as a broadcast device by means of software processes. In addition, a control means possessed by this broadcast device control unit 16 is equipped with a recording control information transmission means in addition to a typical, publicly known control means such as a processing means for the broadcasting of programs.

[0032]

This recording control information transmission means causes the recording control information – which indicates whether group recording of a program stream is permitted – to be included in the program information (hereinafter, 'ECM'), which is one type of control data. The permissibility of group recording is specified freely for each program by the broadcasting company. The ECM describes various information, such as viewing information for each program and a descramble key, and is packetized and multiplexed in the transport stream.

[0033]

Figure 2 is a block diagram showing the configuration of the relevant parts of reception device 3, IC card 4, and VTR 5 in Figure 1.

[0034]

As shown in this figure, reception device 3 has a tuner/demodulation circuit 21, an error correction circuit 22, a signal-processing circuit 23, a separation circuit (DEMUX circuit) 24, a video/audio decoding circuit 25, a video/audio output circuit 26, a mixing circuit 27, a card control unit 28, a connector 29, a control data insertion unit 30, a 1394 interface 31, a user interface (user I/F) 32, and a reception device control unit 33. In addition, tuner/demodulation circuit 21, error correction circuit 22, signal-processing circuit 23, separation circuit (DEMUX circuit) 24, video/audio output circuit 25, video/audio output circuit 26, mixing circuit 27, card

control unit 28, connector 29, control data insertion unit 30, user interface (user I/F) 32, and reception device control unit 33 are interconnected via a bus 34.

[0035]

A broadcast wave is received by an antenna, not shown in the figure, and the broadcast signal is input from a terminal T1 and supplied to tuner/demodulation circuit 21. This broadcast wave is demodulated to a baseband transport stream by tuner/demodulation circuit 21. This demodulated transport stream undergoes a prescribed error correction process at error correction circuit 22 and then is input to signal-processing circuit 23.

[0036]

In signal-processing circuit 23 the descramble key indicated in the ECM included in the transport stream is set by means of reception device control unit 33. The descrambling of the scrambled packets [in] the transport stream is performed in signal-processing circuit 23. Packets to which scrambling has not been applied are [passed] through signal-processing circuit 23 with no processing.

[0037]

The transport stream output from signal-processing circuit 23 is separated into each of its components in DEMUX circuit 24, and of these, the subject matter data are supplied to video/audio decoding circuit 25 while the control data are supplied to reception device control unit 33.

[0038]

The subject matter data are decoded by video/audio decoding circuit 25 and then are supplied to video/audio output circuit 26, where they are appropriately combined and the program data are reproduced. These reproduced program data also are converted to an analog program signal in video/audio output circuit 26 and then this is output from a terminal T2 via mixing circuit 27. A television receiver (not shown in the figure), for example, is connected to terminal T2, and the program is reproduced by this television receiver based on this program signal.

[0039]

Mixing circuit 27 mixes the video signal supplied from reception device control unit 33 with the program signal output from video/audio output circuit 26 so that a menu can be displayed by an OSD (On Screen Display).

[0040]

IC card 4 is installed in reception device 3 by inserting a connector 41 provided on IC card 4 into connector 29. Card control unit 28 is connected to connector 29, and a control circuit 42 is connected to connector 41. Accordingly, when [the IC card] is installed, data are exchanged between card control unit 28 and control circuit 42, thus enabling reception device 3 to access IC card 4.

[0041]

Thus, card control unit 28 exchanges data with control circuit 42 under the control of reception device control unit 33.

[0042]

VTR 5 is connected to reception device 3 by connecting a terminal T11 provided on VTR 5 to a terminal T3 through a cable C. 1394 interfaces 31 and 51, which are provided respectively on reception device 3 and VTR 5, are connected respectively to terminal T3 and terminal T11. Accordingly, when [these components] are connected, data are transmitted between 1394 interfaces 31 and 51 in a procedure in accordance with IEEE 1394, and thus data are exchanged between reception device 3 and VTR 5.

[0043]

The output signal line from 1394 interface 31 to the interior of reception device 3 is connected directly to the data transmission line from error correction circuit 22 to signal-processing circuit 23. Accordingly, the data obtained from VTR 5 by 1394 interface 31 are supplied to signal-processing circuit 23. The input signal line from the interior of reception device 3 to 1394 interface 31 is connected to the data transmission line from error correction circuit 22 to signal-processing circuit 23 via control data insertion unit 30. Accordingly, the transport stream output from error correction circuit 22 is supplied to 1394 interface 31 via control data insertion unit 30 and then is output to VTR 5.

[0044]

Control data insertion unit 30 inserts the EMM supplied from reception device control unit 33 into the transport stream that is transmitted to 1394 interface 31.

[0045]

User I/F 32 inputs signals from an operation panel or a remote control (neither of which is shown in the figure) via a terminal T4, and recognizes the content of instructions from the user. In addition, user I/F 32 notifies reception device control unit 33 of the recognized content of the user instructions.

[0046]

Reception device control unit 33 has a CPU, ROM, and RAM, for example, and implements processes for the overall control of each unit in order to operate as a broadcast device by means of software processes. In addition, a control means possessed by this reception device control unit 33 is equipped with an individual information processing means, a program information processing means, and a control data insertion control means, in addition to a typical, publicly known control means such as a processing means for the reception of programs.

[0047]

The individual information processing means supplies the EMM that has been separated by DEMUX circuit 24 to IC card 4 for [use in] security processes.

[0048]

The program information processing means supplies the ECM that has been separated by DEMUX circuit 24 to IC card 4 for [use in] security processes.

[0049]

When the transport stream is recorded with VTR 5, the control data insertion control means controls control data insertion unit 30 so as to insert the EMM supplied from IC card 4 into the transport stream being recorded.

[0050]

A memory 43 is connected to control circuit 42 of IC card 4. Prescribed information included in the individual information (hereinafter, 'EMM'), such as an ID pertaining to the contract, a descramble key, encoding key, and the like, are registered in memory 43 and are used [sic; possibly, 'this memory is used'] to store prescribed information obtained during operation. When a group setting has been made, an encoding key (hereinafter, 'group key') assigned to the group is registered in addition to a unique encoding key for each contract.

[0051]

Control circuit 42 has a CPU, ROM, and RAM, for example, and performs processes to ensure security pertaining to conditional access reception with reception device 3. The various processing means for the purpose of ensuring this type of security have [sic; possibly, 'include'], a typical, publicly known means for user identification pertaining to the conditional access reception, an individual information storage control means, a recording permissibility judgment means, an individual information generation means, and an encoding means.

[0052]

If the EMM newly received by reception device 3 is for this address, the individual information storage control means updates the information registered in memory 43 to [sic; based on] prescribed information contained in that EMM.

[0053]

Based on the recording control information included in the ECM and the EMM information stored in memory 43, the recording permissibility judgment means judges whether recording of the program stream that has arrived at reception device 3 is permitted and whether group recording is permitted.

[0054]

The individual information generation means uses the information stored in memory 43 to generate EMM for use in group recording only when the recording permissibility judgment means has judged that recording is possible.

[0055]

Then, the encoding means encodes the EMM generated by the individual information generation means. However, when the recording permissibility judgment means has judged that group recording is not permitted and normal recording is required, the encoding means uses a unique key, and when the recording permissibility judgment means has judged that group recording is permitted and group recording is required, it uses the group key.

[0056]

In addition to 1394 interface 51, VTR 5 has recording/reproduction structural unit 52 and a control circuit 53.

[0057]

Recording/reproduction structural unit 52 is formed so as to have a tape drive mechanism and a magnetic head, for example, and a videotape T is mounted therein as needed. In addition, recording/reproduction structural unit 52 records on videotape T the transport stream that is supplied via 1394 interface 51.

[0058]

Control circuit 53 controls 1394 interface 51 and recording/reproduction structural unit 52 to implement the operations of a VTR.

[0059]

Next, the operation of the conditional access system having the aforementioned configuration will be explained.

[0060]

First, when there is a fee for the viewing of a program, the transport stream generated by MUX circuit 12 in broadcast device 1 is scrambled by signal-processing circuit 13.

[0061]

This scrambling occurs in units of packets. The key used for scrambling is a first key ks. This first key ks is changed at a relatively low frequency.

[0062]

Broadcast device control unit 16 indicates the first key ks being used in the ECM. In addition, broadcast device control unit 16 encodes the ECM using a second key kw. This second key kw is changed at a slower frequency than that of the first key ks.

[0063]

Furthermore, broadcast device control unit 16 indicates the second key kw being used in the EMM. Then, broadcast device control unit 16 encodes the EMM using each unique key kmi.

[0064]

The EMM is information that individually reports the information pertaining to a contract on a contract-by-contract basis. Broadcast device control unit 16 sequentially inserts the EMM intended for each contract into the transport stream.

[0065]

The EMM originally is comprised of the basic information I1 shown in Figure 3. This basic information I1 is comprised of subscriber identification information (subscriber ID) I11 and contract setting information I12. Subscriber identification information I11 indicates a unique identifier that is set with respect to the contract for which that EMM is intended. The contract setting information I12 indicates the content of the contract specified by the subscriber identification information I11; however, this contract setting information I12 can be omitted when there is no change in the contract information.

[0066]

However, with the present embodiment, when the contractee has requested a new grouping registration, broadcast device control unit 16 adds group setting information I2 such as that shown in Figure 3 to the EMM pertaining to the contracts to be grouped together.

[0067]

As shown in Figure 3, group setting information I2 includes a group identifier I21 and an encoding key I22. Group identifier I21 is an identifier that is determined so as to be unique to the group. Encoding key I22 is an encoding key that permits shared use [sic; possibly, 'the shared use of which is permitted'] with the multiple contracts included in the group specified by group identifier I21; in other words, it indicates a group key.

[0068]

At reception device 3 the EMM included in the transport stream is extracted by DEMUX circuit 24 and is supplied to control circuit 42 of IC card 4 via card control unit 28 under the control of reception device control unit 33.

[0069]

When control circuit 42 receives the EMM from reception device 3, it judges whether that EMM pertains to its own contract; in other words, it judges the legitimacy of the EMM. If it is confirmed that the EMM is legitimate, the data stored in memory 43 are updated based on each piece of data included in this EMM. Thus, a newly assigned group identifier and group key are registered in IC card 4 and can be subsequently used.

[0070]

Similarly, the EMM indicating the same group identifier and group key is supplied to other contracts that are to be grouped together as the same group G. Accordingly, a shared group

identifier and group key are used among multiple contracts and [thus] a grouping registration is performed.

[0071]

On the other hand, when a program is broadcast, broadcast device control unit 16 creates the ECM for that program and inserts it into the transport stream.

[0072]

The ECM originally is comprised of the basic information I3 shown in Figure 4. This basic information I3 is comprised of viewing information I31 and a descramble key I32. Viewing information I31 includes information indicating program viewing conditions, fee information, and the like, as needed. Descramble key I32 is for the purpose of descrambling the transport stream.

[0073]

However, with the present embodiment, broadcast device control unit 16 adds recording control information I4 such as that shown in Figure 4 to the ECM.

[0074]

As shown in Figure 4, recording control information I4 includes recording permissibility information I41, group recording permissibility information I42, and recording-permitted-group information I43. Recording permissibility information I41 indicates whether recording to videotape T or the like is permitted. Group recording permissibility information I42 indicates whether group recording is permitted. Recording-permitted-group information I43 indicates the group identifier for the group for which group recording is permitted.

[0075]

When a pay-per-view program has been selected at reception device 3, the ECM included in the transport stream is extracted by DEMUX circuit 24 and is supplied to control circuit 42 of IC card 4 via card control unit 28 under the control of reception device control unit 33.

[0076]

When control circuit 42 receives the ECM from reception device 3, it compares the viewing information indicated in that ECM with the contract setting information that has been extracted from the EMM and stored in memory 43 to determine whether this program can be viewed under the terms of this reception device's contract. Then, control circuit 42 notifies

reception device 3 of the judgment result, and when viewing is possible, it also supplies the descramble key to reception device 3. Furthermore, if recording control information is included in the ECM, control circuit 42 supplies this recording control information to reception device 3 in the decoded state.

[0077]

At reception device 3, if a notification that viewing is possible has been provided from IC card 4, then reception device control unit 33 sets that notification and the supplied descramble key in signal-processing circuit 23, and the transport stream is descrambled. Thus, viewing of the pay-per-view program is enabled. Furthermore, if recording control information has been supplied, reception device control unit 33 holds that information in its internal memory. Furthermore, if a notification that viewing is not possible has been provided from IC card 4, reception device control unit 33 does what is necessary – for example, notifying the user of that situation.

[0078]

With the present embodiment, a format is used whereby the transport stream is recorded before descrambling when a program is recorded. Accordingly, even when a program is capable of being viewed based on the aforementioned operation, the program cannot be recorded as is.

[0079]

If a user request for program recording is transmitted via user I/F 32, reception device control unit 33 executes a recording control process such as that shown in Figure 5 in response thereto.

[0080]

In this recording control process, reception device control unit 33 first confirms the recording control information saved in its internal memory (step ST1). In other words, reception device control unit 33 judges whether recording of the program being selected is permitted, and whether group recording is possible, and – when the respective charges for individual recording and group recording differ – it determines how much those charges are. [The term] 'individual recording' means conventional recording in a format whereby the recorded content can be reproduced only on a single reception device 3.

[0081]

Next, reception device control unit 33 creates an image such as that shown in Figure 6, for example, indicating the results of the aforementioned judgments, and outputs this image via mixing circuit 27 for display on a television receiver or the like. At this time the display format can be a format that is displayed in place of the program image, or it can be [a format] based on an OSD.

[0082]

With the example in Figure 6, the program title, recording conditions (in this case it shows that both individual recording and group recording are permitted), and the charges are displayed. Furthermore, buttons B1, B2 and B3 are displayed to enable the user to specify individual recording or group recording or to stop (cancel) the recording of a program.

[0083]

In this state reception device control unit 33 waits for the user to select/specify button B1, B2, or B3, and then checks that input (step ST3). In other words, when selection information indicating either the start of individual recording or group recording or the cancellation of recording is input from user I/F 32, reception device control unit 33 confirms whether the input is correct according to the information being held [in memory].

[0084]

When the input is correct, reception device control unit 33 judges whether it is a request for recording to start (step ST4); otherwise – in other words, when a cancellation has been specified – the recording control process ends in this state.

[0085]

However, if the start of recording has been requested, reception device control unit 33 operates card control unit 28 and requests that IC card 4 confirm the contract information (step ST5).

[0086]

When this request is received and if it has been reported that group recording is to be performed, control circuit 42 of IC card 4 confirms whether a group identifier and a group key have been set in memory 43. When a group identifier and a group key have not been set in memory 43, control circuit 42 transmits a reply to reception device 3 indicating that group

recording is not possible; when a group identifier and a group key have been set in memory 43, it transmits a reply indicating that group recording is possible.

[0087]

Thus reception device control unit 33 confirms the responses from IC card 4 and judges whether recording of the program requested by the user can be performed (step ST6). When recording of the program cannot be performed as requested, reception device control unit 33 outputs, via mixing circuit 27, an image for the purpose of notifying the user of that situation, and thus displays [the image] in a television receiver or the like (step ST7), and then the current recording control process ends. Figure 7 is an example of the images displayed when the grouping [sic] required for recording of the program being selected has not been registered.

[0088]

On the other hand, if recording of the program as requested can be performed, reception device control unit 33 judges whether individual recording or group recording is to be performed (step ST8). If individual recording is to be performed, IC card 4 is requested to create EMM for use with individual recording (step ST9), and if group recording is to be performed, [IC card 4] is requested to create EMM for use with group recording (step ST10).

[0089]

When the creation of EMM for recording use is thus requested, control circuit 42 in IC card 4 uses the data stored in memory 43 to create the EMM. When [EMM] for use in individual recording has been requested, a unique key is used to encode the aforementioned EMM that has been created, and when [EMM] for use in group recording has been requested, a group key is used. Then, control circuit 42 supplies this encoded EMM to reception device 3.

[0090]

Then, reception device control unit 33 supplies the EMM, which has been supplied from IC card 4 as described above, to control data insertion unit 30, where it is inserted into the NULL packet portion of the transport stream (step ST11), after which reception device control unit 33 ends the current recording control process.

[0091]

The transport stream in which the EMM has been inserted by control data insertion unit 30 undergoes a format conversion in 1394 interface 31 and then is output from terminal T3 in the scrambled state.

[0092]

At VTR 5 the transport stream that has been output from terminal T3 of reception device 3 and transmitted via cable C is picked up by 1394 interface 51 and recorded on videotape T by recording/reproduction structural unit 52.

[0093]

Thus, a transport stream into which the EMM generated by IC card 4 has been inserted is output to VTR 5, and this transport stream is recorded on videotape T.

[0094]

The operation for viewing of a program based on the transport stream recorded on videotape T is as follows.

[0095]

First, the transport stream recorded on videotape T is read out by recording/reproduction structural unit 52 and supplied via 1394 interface 51 to reception device 3 via cable C.

[0096]

At reception device 3 the transport stream thus supplied from VTR 5 is picked up by 1394 interface 31 and supplied as is to signal-processing circuit 23. Then, reproduction of the program based on this transport stream supplied from VTR 5 occurs in the same manner as when a broadcast is received, but the EMM used in this case has been generated by IC card 4 when [the program was] recorded.

[0097]

When this EMM has been encoded using a unique key, the release of that encoding is [enabled] only with the IC card 4 that was installed in the reception device 3 that received the transport stream when the program was recorded. Accordingly, reception device 3 is able to obtain the descramble key, and the program can be reproduced only, when the same IC card 4 that was used to record the program is installed in reception device 3.

[0098]

In contrast thereto, when the EMM has been encoded using a group key, the release of the encoding is [enabled] only with an IC card 4 that has been registered in the same group as the IC card 4 that was installed in the reception device 3 that received the transport stream when the

program was recorded. Accordingly, even if an IC card 4 other than the one used when the program was recorded is installed in reception device 3, the program can be reproduced as long as the installed IC card 4 is registered in the same group as [the IC card] used when the program was recorded.

[0099]

Thus, by means of the present embodiment, a shared group key is registered with respect to multiple IC cards 4, and when group recording is performed, the EMM that has been encoded using the group key is inserted into the transport stream to be recorded. Accordingly, reproduction of a program based on a transport stream for which group recording has been performed can occur in any reception device 3 in which [any of] the multiple IC cards 4 for which the shared group key has been registered is installed. Consequently, it is possible to view [a program] using a reception device 3 other than the one with which the program was recorded without having to exchange IC card 4, which significantly improves the user's convenience. In other words, for example, if there are multiple reception devices 3 in one home, then by registering the respective contracts pertaining to those reception devices 3 as a group, it becomes possible to view a program recorded in one room in another room, which increases the user's degree of freedom with respect to viewing.

[0100]

Furthermore, with the present embodiment, the viewing range for a program for which group recording is permitted is restricted to [reception devices for which] the same group registration has been performed, so it is possible to prevent abuse such as the distribution of copies, and security can be sufficiently maintained.

[0101]

Furthermore, by means of the present embodiment, group recording can be used effectively only with contracts for which a group registration has been performed, so the broadcasting company also is able to recover a charge for a service whereby the registration of groups is permitted.

[0102]

Moreover, by means of the present embodiment, the ECM is used to report the recording control information I4 from broadcast device 1 to reception device 3, so recording control information I4 is reported during broadcasting as frequently as approximately every 100 ms to several seconds. Accordingly, recording control information I4 can be obtained quickly at

reception device 3 at any time during the program broadcast, and a judgment regarding whether recording is permitted can be made in real time when it becomes necessary to record a program.

[0103]

Furthermore, the present invention is not limited to the aforementioned embodiment. For example, with the aforementioned embodiment, the recording control information I4 is transmitted from broadcast device 1 to reception device 3 by including it in the ECM; however, it also can be included in the control information that constitutes the program guide information, such as an EIT (Event Information Table) or SDT (Service Definition Table). Figure 8 is a diagram showing the situation when recording control information I4 is included in an EIT. In this figure the symbol I5 denotes the program structural component data, which is the basic information of the EIT, and the recording control information I4 has been included by appending it thereto.

[0104]

If recording control information I4 is thus included in the program guide information, the permissibility of group recording can be judged before the program broadcast begins, and for example the recording method can be selected when a reservation for a timer recording is made.

[0105]

However, in this case the EMM for recording use is supplied from IC card 4 before the program broadcast begins, so that the EMM will be stored and held in reception device 3 until the program actually is broadcast. Alternatively, the recording request from the user can be held in reception device 3 until the program broadcast begins, and broadcast device 1 can request the EMM from IC card 4 when the broadcast starts or just before the broadcast starts.

[0106]

Program guide information such as in the EIT is not characterized by being real-time [information], but it is information that can be obtained in all time slots, and the ECM is information that can be obtained in real time at short intervals while the program is being broadcast; therefore, by reporting the recording control information I4 with both of these types of control information, the recording control operation can be performed smoothly at any time, from the time of the [recording] reservation to [a time] during the broadcast of the program.

[0107]

Furthermore, recording control information I4 can be included in preexisting control information other than the ECM, EIT [information], or SDT [information]; or, a specific type of control data for the purpose of reporting the recording control information I4 can be established and can be transmitted as a suitable packet.

[0108]

Furthermore, with the aforementioned embodiment, reception device 3 outputs the transport stream for recording use to a separate VTR 5, with VTR 5 recording [the program] to videotape T, but the functionality of VTR 5 can be embedded in reception device 3.

[0109]

Furthermore, with the aforementioned embodiment, videotape T was used as an example of the recording medium for recording of the program, but any recording medium, such as a DVD, can be used.

[0110]

Various other embodiments are possible without departing from the scope of the present invention.

[0111]

Effect of the invention

By means of the present invention, group recording is enabled according to the user's desire only for programs for which it is indicated – by means of the recording control information indicated in the program stream at the broadcast device – that group recording is permitted; in addition, this group recording is performed by recording a recording-use program stream formed by multiplexing individual information – which is generated by the security module and has been encoded using a prescribed encoding key that is shared by multiple contracts – with the aforementioned program stream transmitted from the broadcast device. Therefore, the degree of freedom can be improved with respect to reproduction of programs recorded on a recording medium within a prescribed region, such as a home, and convenience can be ensured for the subscriber, while preventing abuse such as the distribution of copies.

Brief description of the figures

Figure 1 is a block diagram showing the configuration of the relevant parts of a conditional access system and the relevant parts of a broadcast device according to an embodiment of the present invention.

Figure 2 is a block diagram showing the configuration of the relevant parts of reception device 3, IC card 4, and VTR 5 in Figure 1.

Figure 3 is a diagram schematically illustrating the configuration of the EMM data used with an embodiment of the present invention.

Figure 4 is a diagram schematically illustrating the configuration of the ECM data used with an embodiment of the present invention.

Figure 5 is a flowchart showing the processing procedure when recording control is performed by reception device control unit 33 in Figure 1.

Figure 6 is a diagram showing one example of an image displayed to present information pertaining to the recording of a program to the user.

Figure 7 is a diagram showing one example of an image displayed to notify the user that group recording cannot be performed.

Figure 8 is a diagram showing an example wherein the recording control information is included in an EIT.

Explanation of symbols

1	Broadcast device
3	Reception device
4	IC card
11	Video/audio encoding circuit
12	Multiplexing circuit (MUX circuit)
13	Signal-processing circuit
14	Error correction-encoding circuit
15	Modulation circuit
16	Broadcast device control unit
30	Control data insertion unit
33	Reception device control unit
42	Control circuit
43	Memory
T	Videotape

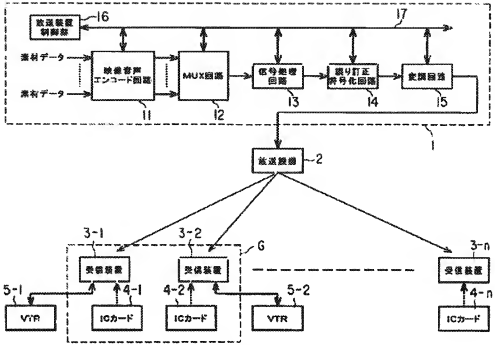


Figure 1

Key:

1	Subject matter data
2	Broadcast device
3-1, 3-2, 3-n	Reception device
4-1, 4-2, 4-n	IC card
11	Video/audio encoding circuit
12	MUX circuit
13	Signal-processing circuit
14	Error correction-encoding circuit
15	Modulation circuit
16	Broadcast device control unit

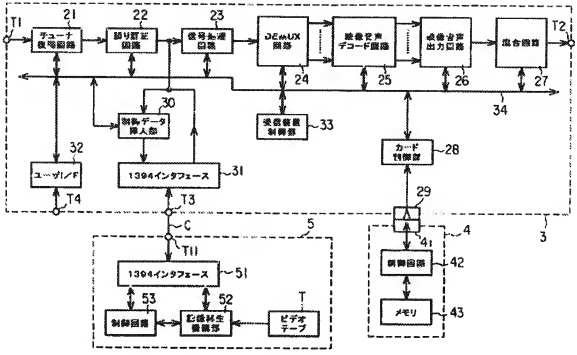


Figure 2

Key:
- 21 Tuner/demodulation circuit
- 22 Error correction circuit
- 23 Signal-processing circuit
- 24 DEMUX circuit
- 25 Video/audio decoding circuit
- 26 Video/audio output circuit
- 27 Mixing circuit
- 28 Card control unit
- 30 Control data insertion unit
- 31 1394 interface
- 32 User I/F
- 33 Reception device control unit
- 42 Control circuit
- 43 Memory
- 51 1394 interface
- 52 Recording/reproduction structural unit
- 53 Control circuit
- T Videotape

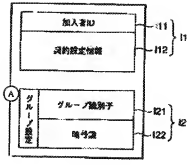


Figure 3

Key: A Group setting
I11 Subscriber ID
I12 Contract setting information
I21 Group identifier
I22 Encoding key

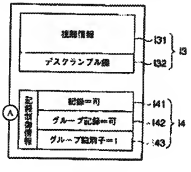


Figure 4

Key: A Recording control information
I31 Viewing information
I32 Descramble key
I41 Recording = Permitted
I42 Group recording = Permitted
I43 Group identifier = 1

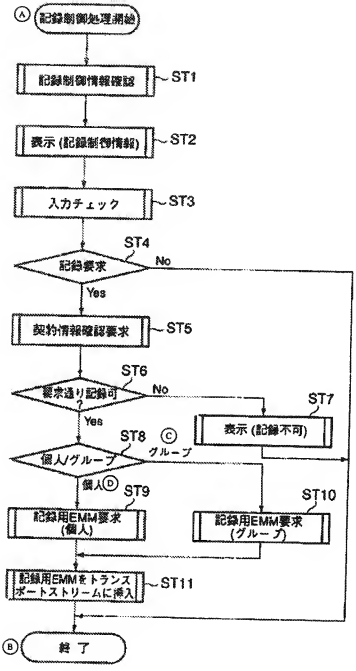


Figure 5

Key: A Recording control process starts
B End
C Group
D Individual
ST1 Confirm recording control information

ST2 Display (recording control information)
ST3 Check input
ST4 Recording request?
ST5 Request confirmation of contract information
ST6 Recording as requested possible?
ST7 Display (recording not possible)
ST8 Individual/Group?
ST9 Request EMM for recording use (individual)
ST10 Request EMM for recording use (group)
ST11 Insert EMM for recording use into transport stream

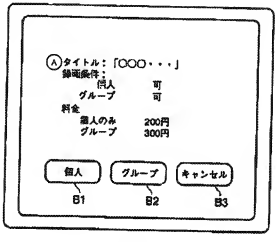


Figure 6

Key: A Title:
Recording conditions:
Individual – Permitted
Group – Permitted
Charge
Individual only – 200 yen
Group – 300 yen
B1 Individual
B2 Group
B3 Cancel

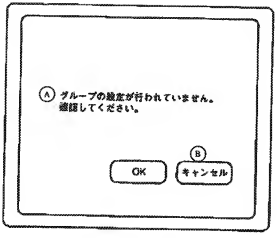


Figure 7

Key: A No group setting has been made. Please confirm.
B Cancel

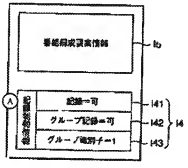


Figure 8

Key: A Recording control information
I5 Program structural component information
I41 Recording = Permitted
I42 Group recording = Permitted
I43 Group identifier = 1

Continued from front page

(51) Int.Cl.[7]	Identification Codes	FI			(Reference)
H 04 N 5/44		H 04 N	5/44	Z	
		H 04 L	9/00 601	C	
7/025		H 04 N	7/08	A	
7/03					
7/035					

F Terms (Reference)

5C025 AA25 AA30 BA25 BA27 BA30
CB07 CB10 DA01 DA05 DA10
5C063 AA20 AB03 AB07 AC01 AC05
AC10 CA11 CA40 DA20
5C064 BA01 BB01 BB02 BC06 BC16
BC20 BC22 BC25 BC27 BD09
5J104 AA01 AA16 AA32 BA03 EA02
EA17 NA02 NA35 NA41 PA05
9A001 BB03 CC05 DD13 EE03 HH35
JJ71 KK56 KK62 LL03 LL07
LL09